How secure are our industrial control systems?

Hendrik Derre
Hendrik Derre

◦ Research associate at Howest University with the ‘Security & Privacy Research Group’
◦ Master’s degree in engineering technologies
◦ Specialized in ICS security

---

**Education - Research - Consulting**

- GDPR
- Blockchain
- Cyber Security
Security?
What not to fear...
What should you be worried about…

Your personal files are encrypted!

Your important file encryption produced on this computer’s photos, videos, documents, etc. [link] is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key [RSA 2048] generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files.

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR and a similar amount in another currency.

Click [Next] to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate...

Ransomware spiked 6,000% in 2016 and most victims paid the hackers, IBM finds

Harriet Taylor | @HarrietT
Wednesday, 14 Dec 2016 10:00 AM ET

One of Europe’s top hotels has admitted they had to pay thousands in Bitcoin ransom to cybercriminals who managed to hack their electronic key system, locking hundreds of guests out of their rooms until the money was paid. (Updated)
What should you be worried about...

1 Tbps DDoS Attack
Powered By 150,000 Hacked IoT Devices

BrickerBot: Mirai-like malware threatens to brick insecure IoT devices
PDos attack could render your Linux-based IoT devices useless
**Smart Buildings**

**A Back Door for Hackers?**

Connected Building Systems Fly under the Cybersecurity Radar, Creating "Shadow IoT"

---

**What should you be worried about...**

---

**Hello, Iam Idahc a Lebanese Hacker**

I was Bored and I play the game of the year: "hacker vs Sony"

I hacked little database of 120 user with an sql injection......

site:http://apps.pro.sony.eu/

---

<table>
<thead>
<tr>
<th>username</th>
<th>password</th>
<th>mobile</th>
<th>office</th>
<th>email</th>
<th>website</th>
</tr>
</thead>
<tbody>
<tr>
<td>scul +44 7818 0</td>
<td>dam83d</td>
<td>18</td>
<td>go</td>
<td>csie.unav</td>
<td>es</td>
</tr>
<tr>
<td>JafarAbd ourfar</td>
<td>1458999</td>
<td>15222</td>
<td>qour@pendarfi</td>
<td>hister@ingenio</td>
<td>techiniche.com</td>
</tr>
<tr>
<td>arth +44 7887 8</td>
<td>44 788</td>
<td>91 63</td>
<td>63</td>
<td>yahoo.es</td>
<td>google.com</td>
</tr>
<tr>
<td>o alro +44 07592</td>
<td>44 (6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bern +34 630 163</td>
<td>91 63</td>
<td>63</td>
<td>63</td>
<td>yahoo.es</td>
<td>google.com</td>
</tr>
<tr>
<td>marie c68763c0c7</td>
<td>465cfd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the Argthe +3069</td>
<td>+3069</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>van vanbar +32 47</td>
<td>5 +32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>loc locbon +44 (6)</td>
<td>66545</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mal malbru +33 6</td>
<td>8 +33</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Johansen senato</td>
<td>91355</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**GDPR**

EU General Data Protection Regulation
The weakest Link.... ICS?
Industrial Control System Vulnerabilities

- System Vulnerabilities
- Network Vulnerabilities
- Policy and Procedure Vulnerabilities
System Vulnerabilities

- **Architecture and Design Vulnerabilities**
  - Inadequate incorporation of security into architecture and design.
  - Control network services not within a separate control network.

- **Configuration and Maintenance Vulnerabilities**
  - OS and application security patches are not maintained.
  - Passwords generation, use, and protection not in accord with policy.
  - Malware protection not installed or up to date.

- **Physical Vulnerabilities**
  - Unauthorized personnel have physical access to equipment.
  - Inadequate authentication, privileges, and access control in software.
System Vulnerabilities

- **Architecture and Design Vulnerabilities**
  - Inadequate incorporation of security into architecture and design.
  - Control network services not within a separate control network

- **Configuration and Maintenance Vulnerabilities**
  - OS and application *security patches* are not maintained
  - Passwords generation, use, and protection not in accord with policy
  - Malware protection not installed or up to date

- **Physical Vulnerabilities**
  - Unauthorized personnel have physical access to equipment
  - Inadequate authentication, privileges, and access control in software
ICS-CERT Alerts
An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.
[change view]: Alerts by Vendor

- ICS-ALERT-17-089-01: Miele Professional PG 8528 Vulnerability
- ICS-ALERT-17-073-01: MEMS Accelerometer Hardware Design Flaws
- ICS-ALERT-16-286-01: Sierra Wireless Mitigations Against Mirai Malware
- ICS-ALERT-16-253-01: BINOM3 Electric Power Quality Meter Vulnerabilities
- ICS-ALERT-16-256-01: FENIKS PRO Elnet Energy Meter Vulnerabilities
- ICS-ALERT-16-256-02: Schneider Electric ION Power Meter CSRF Vulnerability
- IR-ALERT-L-16-230-01: Navis WebAccess SQL Injection Exploitation
- ICS-ALERT-16-230-01: Navis WebAccess SQL Injection Vulnerability
- ICS-ALERT-16-182-01: Sierra Wireless AirLink Raven XE and XT Gateway Vulnerabilities
- ICS-ALERT-16-099-01B: Moxa NPort Device Vulnerabilities (Update B)

https://ics-cert.us-cert.gov/alerts
System Vulnerabilities

- **Architecture and Design Vulnerabilities**
  - Inadequate incorporation of security into architecture and design.
  - Control network services not within a separate control network

- **Configuration and Maintenance Vulnerabilities**
  - OS and application security patches are not maintained
  - Passwords generation, use, and protection not in accord with policy
  - Malware protection not installed or up to date

- **Physical Vulnerabilities**
  - Unauthorized personnel have physical access to equipment
  - Inadequate authentication, privileges, and access control in software
System Vulnerabilities

🔹 **Architecture and Design Vulnerabilities**
  - Inadequate incorporation of security into architecture and design.
  - Control network services not within a separate control network

🔹 **Configuration and Maintenance Vulnerabilities**
  - OS and application security patches are not maintained
  - **Passwords generation**, use, and protection not in accord with policy
  - Malware protection not installed or up to date

🔹 **Physical Vulnerabilities**
  - Unauthorized personnel have physical access to equipment
  - Inadequate authentication, privileges, and access control in software
System Vulnerabilities EXAMPLES

Password Generation

25. Create a new user account. For user name use _ and password _
   Click the Add to list button.
System Vulnerabilities

- **Architecture and Design Vulnerabilities**
  - Inadequate incorporation of security into architecture and design.
  - Control network services not within a separate control network.

- **Configuration and Maintenance Vulnerabilities**
  - OS and application security patches are not maintained.
  - Passwords generation, use, and protection not in accord with policy.
  - Malware protection not installed or up to date.

- **Physical Vulnerabilities**
  - Unauthorized personnel have physical access to equipment.
  - Inadequate authentication, privileges, and access control in software.
System Vulnerabilities

Architecture and Design Vulnerabilities
- Inadequate incorporation of security into architecture and design.
- Control network services not within a separate control network

Configuration and Maintenance Vulnerabilities
- OS and application security patches are not maintained
- Passwords generation, use, and protection not in accord with policy
- Malware protection not installed or up to date

Physical Vulnerabilities
- Unauthorized personnel have physical access to equipment
- Inadequate authentication, privileges, and access control in software
Physical Vulnerabilities
Physical Vulnerabilities


2.27.8 Switch Keys

The key switches required by 2.27.2 through 2.27.5 for all elevators in a building shall be operable by the same key. The keys shall be Group 3 Security (see 8.1). There shall be a key for each switch provided. These keys shall be kept on the premises in a location readily accessible to firefighters and emergency personnel, but not where they are available to the public.

This key shall be of a tubular, 7 pin, construction and shall have a bitting code of 6143521. The key shall be coded "FFE-K1."

The possession of the “FFE-K1” key is limited to elevator personnel, emergency personnel and elevator equipment manufacturers. Where practical, the lock, including its lock and other components, shall conform to the requirements of UL 1033.

NOTE (2.27.8): Local authorities may impose additional requirements for a uniform keyed lock box and its location to contain the necessary keys.
Physical Vulnerabilities

Welcome to ElevatorKeys.com!

ElevatorKeys.com is the leading online retailer of elevator keys and access control solutions, exclusively serving authorized persons as defined by code. We also offer special order key switches, access control systems, integration services, and elevator security consulting services.

Our personal customer service is just one part of our effort to make sure every customer is completely satisfied. We want you to think of ElevatorKeys.com any time you have a need for elevator keys or key switches. If you have a special need for something you don't see on our site, contact us for more information or call +1 (855) 469-8364.
System Vulnerabilities

Examples

Physical Vulnerabilities

ElevatorKeys.com

CCL BG390 key for Otis elevators
CCL BG390 key for Otis elevators. May also be marked "CCL BG390" or "3000" BG390"... $3.99

Otis UTA key
UTA key for Otis Elevators, found on many contemporary styles of Otis fixtures...
$4.99

UTB key for Otis Elevators, found on many contemporary styles of Otis fixtures...
$4.99

UTC key for Otis Elevators, found on many contemporary styles of Otis fixtures...
$4.99
System Vulnerabilities

Examples

Physical Vulnerabilities
Industrial Control System Vulnerabilities

- System Vulnerabilities
- Network Vulnerabilities
- Policy and Procedure Vulnerabilities
Network Vulnerabilities

- **Protocol Vulnerabilities**
  - Use of unsecure industry-wide ICS protocols
  - Authentication? Integrity? Confidentiality?
  - Standard, well-documented communication protocols are used

- **Network architecture Vulnerabilities**
  - Firewalls nonexistent or improperly configured
  - No intrusion detection systems
  - Use of wireless communication with inadequate data protection
Network Vulnerabilities EXAMPLES

https://www.shodan.io/
Network Vulnerabilities EXAMPLES

Do Not Try This at Home
Industrial Control System Vulnerabilities

System Vulnerabilities

Network Vulnerabilities

Policy and Procedure Vulnerabilities
Policy and Procedure Vulnerabilities

- Inadequate security policy for the ICS
- No formal ICS security training and awareness program
- Lack of administrative mechanisms for security policy enforcement
- Inadequate incident detection and response plan and procedures
- Inadequate review of the effectiveness of the ICS security controls
Industrial Control System Vulnerabilities

- System Vulnerabilities
- Network Vulnerabilities
- Policy and Procedure Vulnerabilities
Cybersecurity Security Frameworks

WHAT TO DO NEXT...
Build a Information Security Management System

“An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.” – ISO/IEC 27001
Build a Information Security Management System

- Do risk assessment
Build a Information Security Management System

Use a Cybersecurity Framework (eg. NIST)
Cybersecurity Security Frameworks

Build a Information Security Management System

- Adapt the Framework for ICS
  http://isa99.isa.org
Build a Information Security Management System

Adapt the Framework for ICS

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
Get Expert Advice!

- We are happy to help...so contact us!! 🌟
  - Training (on-site possible)
  - Security & Privacy Audits
Thank you!
Any Questions?

hendrik.derre@howest.be
www.linkedin.com/in/hendrikderre
@derre_h
ELA 2017 CONFERENCE

Lifts & Escalators – our part in the Digital World

Radisson Blu Hotel, Luzern